



## Industry

# GLOBAL MANUFACTURING COMPANY

40 global Branches  
EMPLOYEES - 10000+

## CASE STUDY

A global manufacturing Company was facing major cybersecurity challenges and LinkShadow had the opportunity to collaborate to help them enhance and secure their security environment.

## CHALLENGES

**With offices spread across multiple countries, some of the major challenges that the LinkShadow team identified were the following:**

- With a highly customised environment traditional threat detection platform were falling short to successfully identify threats.
- Unable to detect and respond to cyber threats quickly and effectively manage vulnerabilities across the organisations networks, systems, and applications from every office location.
- The need to implement monitoring and access controls for employees to safeguard sensitive information and systems.
- Risks from exposure to external vendors introducing additional security risks. There was a need to implement strict security standards and controls to mitigate risks.
- Need to deploy cybersecurity regulations and standards to ensuring compliance.



## SOLUTION

LinkShadow deployed its sensors in all the branch offices across the globe and a main management appliance in the HQ from where their analyst could monitor and manage the threats. A customized platform according to their infrastructure needs was deployed to deliver Threat Management and Visibility. LinkShadow intelligent NDR and UEBA helped the customer mitigate the risks associated with cyber threats.

- With advanced threat detection capabilities LinkShadow enabled to identify potential threats and vulnerabilities across the organization's networks, systems, and applications. Also helped monitor for suspicious behaviour and anomalies, detect and alert on targeted attacks, and identify advanced threats like malware and ransomware.
- Helped provide visibility into user behavior of employees and vendors to identify suspicious activities and generate alerts in real-time.
- Helped meet with the regulatory requirements and standards related to cyber security by providing a comprehensive approach to cyber security analytics. Linkshadow provided visibility into compliance with regulations and standards, generate compliance reports, and help to demonstrate compliance to auditors.

## CUSTOMER FEEDBACK

"Implementing the LinkShadow iNDR and UEBA solution significantly improved the security status by providing advanced threat detection, incident response, data protection, insider threat detection, and compliance capabilities protect against cyberattacks and minimize the impact of security incidents."



## BENEFITS

The customer was able to obtain central visibility of Traffic - Threats from all the branches across the globe from a central management appliance in HQ.

LinkShadow iNDR and UEBA provided customer with enhanced threat detection capabilities that helped detect potential threats across the organization's networks, systems, and applications. iNDR detects network-based threats, while UEBA helps identify unusual user behaviour that could be indicative of an attack.

Achieved faster incident response by providing automated incident response capabilities that helped quickly remediate threats before they can cause damage or data loss. Customer could leverage the solution's automated response capabilities to reduce the time to resolution and minimize the risk of damage or data loss.

Enabled adoption of a more proactive approach to cyber security by identifying and remediating security risks before they can be exploited by attackers.

Helped improve visibility into its security posture, including the ability to monitor and analyze user behaviour, network traffic, and system activity. The solution's advanced analytics capabilities provided the SOC analysts with actionable intelligence to improve its security posture.